



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/884,672

06/19/2001

Tetsuya Noguchi

JP920000134US1

4503

7590

03/14/2006

IBM CORPORATION
INTELLECTUAL PROPERTY LAW DEPT.
P.O. Box 218
YORKTOWN HEIGHTS, NY 10598

EXAMINER

POLTORAK, PIOTR

ART UNIT

PAPER NUMBER

2134

DATE MAILED: 03/14/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/884,672	NOGUCHI ET AL.	
	Examiner	Art Unit	
	Peter Poltorak	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 05 December 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-4, 6-16, 18-28 and 30-41 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-4, 6-16, 18-28 and 30-41 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. The Amendment, and remarks therein, received on 12/5/2005 have been entered and carefully considered.
2. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior office action.

Response to Amendment

3. Applicant's arguments have been carefully considered.
4. Applicant argues that Vainio does not teach that two send/receive devices generate verification data and send that data to their respective output devices, after which the data are compared. Later on applicant similarly argues that Vainio does not teach SRES values that are placed in verification data output section.
5. Applicant's arguments have been carefully considered but they were not found persuasive. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., SRES values that are placed in verification data output section) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).
6. However, Vainio does teach "generating verification data from the sent data for verification data generation ... and outputting the generated verification data to its own verification data output section".

7. Vainio teaches data for verification data generation (RAND A) from one data send/receive device to the other send/receive device, wherein the two send/receive devices are mutually connected by an ad-hoc radio connection (*In Vanios' Bluetooth authentication scheme a Device A sends RAND A to a Device B. 5.3 Authentication, in particular Fig. 6*).
8. Vainio teaches generation in the one data send/receive device, generating verification data (SRES') from the sent data for verification data generation produced using a first generation algorithm (E1) and outputting the generated verification data (*5.3 Authentication, illustrated by Fig. 1, in particular the Device A*).
9. Vainio also teaches in the other data send/receive device, generating verification data (SRES) from the received data for verification data generation produced using the first generation algorithm (E1) and outputting the generated verification data to its own verification data output section (*5.3 Authentication, illustrated by Fig. 1, in particular the Device B*).
10. Vainio teaches comparing the verification data for mutual matches ($SRES' \neq SRES$, *Fig. 6*).
11. Applicant argues that the generation of a plurality of verification data values for example for data having a plurality of divisions is neither taught nor suggested and pointed to page 23.
12. Applicant's arguments have been carefully considered but they were not found persuasive. The examiner points out that "a plurality of divisions" is not recited in the claimed language. Furthermore pages 23 does not clarify the issue of the plurality of

verification data. It is not clear, for example, whether applicant treats "histogram" as a plurality ("of divisions") of verification data, whether the verification data generated with the first generation algorithm on multiple devices qualifies as a plurality of verification data or whether applicant assumed some other interpretation of the limitation.

13. Applicant argues that Vainio does not teach steps for establishing a serial sequence of operators, and letting an input to the serial sequence of operators be the data for verification (*claims 4, 6, 16, 18 and 28*). Later on (pg. 32) applicant reiterates the position and arguing Schneier's complementing Vainio's teaching of the one-way hash functions used in establishing a serial sequence of operators for verification data generation as claimed.
14. Applicant's arguments have been carefully considered but they were not found persuasive. In addressing the actual claim language ("*establishing a serial sequence of operators that are composed of more than one operators arranged in series, wherein the operators relate to the same or different one-way function*") the examiner pointed out that Vainio's teaching discloses data for verification data generation (*RAND A*) being an input to a first generation algorithm (*E1*) that results in an output of the generated verification data.
15. Schneier's discloses a serial sequence of operators that are composed of more than one operators arranged in series (pg. 351-353) that are related to the same or different one-way function.

16. Applicant acknowledges Schneier's teaching presented on pg. 35 but disagrees with the examiner's interpretation of Schneier's teaching. Unfortunately, applicant does not provide any specifics. For applicant convenience the examiner provides additional teaching of one-way function taught by Schneier disclosed on pg. 433-438. Applicant may want to pay particular attention to Fig. 18.2-Fig. 18.5 that more intuitively illustrate the relevance of one-way hash functions to applicant's claimed language.
17. Applicant argues the relevance of Official Notice and states that "while audio and visual prompts and messages may be known, applicant contend that such prompts are not the same as nor suggestive of audible or visual verification data per se".
18. Applicant's arguments have been carefully considered but they were not found persuasive.
19. The example of Windows invalid password was to illustrate that visual output (as well as audible output) is old and well known in the computing arts to report computer particular events to a user. Consider hand held device synchronization that results in data to be displayed on both devices in addition often alerting users about the synchronization success and/or failure.
20. Applicant argues that Vanio and Schneier don't disclose features of claims 8 and 20, in particular that they disclose that a public key may require verification.
21. In order to address applicant argument, in this Office Action the examiner presents Vanio and Schnier's teaching regarding claim 8 and 20 using more clear approach.

22. Lastly, applicant's argument that *Davis* and *Narayanaswami* and *Lin* art would not be appropriate to arrive at the invention as claimed simply because none of these references teaches or suggests the means and steps for generating a plurality of verification data... etc. is not understood since the presented art even though not the same is analogues and complementary to *Vanio's*.

23. Claims 1-4, 6-16, 18-28 and 30-41 have been examined.

Claim Rejections - 35 USC § 112

24. Claims 9- 23 are rejected under 35 U.S.C. 112, second paragraph, as failing to set forth the subject matter which applicant(s) regard as their invention.

25. "The sections of both the data sections" in claims 1 and 13 and "the other" in claims 13 and 25 lack antecedent basis.

26. Claims 13-20 are method claims but a dependent claim 21 is a product claim.

27. Claim 13 recites "determining whether the verification data at the sections of both the data sections of both the data send/receive devices matches mutually".

28. Claim 13 recites: "the plurality of verification data". It is not clear, for example, whether applicant treats "histogram" as a plurality ("of divisions") of verification data (*see the Specification, pg. 23*), whether the verification data generated with the first generation algorithm on multiple devices qualifies as a plurality of verification data or whether applicant assumed some other interpretation of the limitation. For purposes of further examination the phrase is treated as best understood.

29. Claims 9, 11, 21 and 23-24 recite “**the** portable terminal” transmitting the public key to the personal computer of each user (*e.g. claim 9, pg. 7 line 5*). It is not clear which of the portable terminal (“of the one user” or “of the other user”) transmits the public key.

Similarly, in claims 12, 22 it is not clear which of the personal terminal transmits the symmetric key to the personal computers. Furthermore, although the claim language recites both personal terminals obtaining the symmetric key the claim language recite only the personal computers utilizing the symmetric key. As a result it is not clear, for example, whether limitation is missing or whether claims should be understood as both personal terminals transmit the symmetric key to the personal computers.

30. Furthermore claim 9 seems to be missing a limitation. The public key is sent to the personal of each user but the claim language discusses only the computer of the other user utilizing the public key (*“information... transmitted from the personal computer of the other user in cipher using the public key”, pg. 7 lines 10-15*)).

31. Also, a symmetric key K_c is produced using a second generation algorithm. However, it is not clear whether the same data is used on both personal computers to derived K_c since in the claim language only one of the personal computers generates this K_c with additional data (*e.g. a random number*) .

32. Lastly, the additional data is encrypted with the public key (*“information... transmitted from the personal computer of the other user in cipher using the public key”, pg. 7 lines 10-15*)). However there is no step of decryption and it is not even

Art Unit: 2134

clear how the encrypted data is retrieved since there is no information regarding the decrypted key.

33. Similar ambiguity is observed in claims 11, 21 and 23.

34. Applicant should rewrite the claim language so that the metes and bounds are unambiguous.

35. Claims 10, 12, 21 recite: "and wherein each personal computer comprises means to generate a symmetric key Kc such that the portable terminal of the other user generates a symmetric key Kc produced using ..., while the portable terminal of the one user generates the symmetric key Kc...".

The recitation is not clear. Each personal computer generates a symmetric key such that the portable terminals generate a symmetric key Kc. The connection between a symmetric key generated by each personal computer and each portable terminal is not understood. Furthermore, it is not understood whether the term "while" is used as equivalent of "and" or whether the limitation attempts to contrast the symmetric keys produced by two different portable terminals.

36. Claims 33-35 and 37-39 are rejected by virtue of their dependence.

Appropriate correction is required

Claim Rejections - 35 USC § 102

37. Claims 1, 13, 25, 30-31 and 37 are rejected under 35 U.S.C. 102(e) as being anticipated by Vainio (Juha T. Vainio, "Bluetooth Security").

38. Vainio teaches sending data for verification data generation (RAND A) from one data send/receive device to the other send/receive device, wherein the two send/receive

devices are mutually connected by an ad-hoc radio connection (*In Vanios' Bluetooth authentication scheme a Device A sends RAND A to a Device B. 5.3 Authentication, in particular Fig. 6*).

39. Vainio teaches in the one data send/receive device, generating verification data (*SRES'*) from the sent data for verification data generation produced using a first generation algorithm (*E1*) and outputting the generated verification data (5.3 *Authentication, illustrated by Fig. 1, in particular the Device A*).
40. Vainio also teaches in the other data send/receive device, generating verification data (*SRES*) from the received data for verification data generation produced using the first generation algorithm (*E1*) and outputting the generated verification data to its own verification data output section (5.3 *Authentication, illustrated by Fig. 1, in particular the Device B*).
41. Vainio teaches determining whether the verification data at the sections of both the data sections of both the data send/receive devices matches mutually (*SRES' ?= SRES, Fig. 6*).
42. Vainio's invention is a generic discussion clearly intended to multiple use in multiple devices and as a result the authentication scheme as disclosed in Fig. 6 is repeated numerous times resulting in generation of a plurality of verification data values that is then matched (*SRES?=SRES'*). Thus, Vainio teaches the first generation algorithm generating a plurality of verification data, wherein for each verification data, it is determined whether the verification data at the verification data output sections of both the data send/receive devices match mutually.

Art Unit: 2134

43. Claims 1, 25 and 30-31 are substantially equivalent to claim 13; therefore claims 1, 25 and 30-31 are similarly rejected.

Claim Rejections - 35 USC § 103

44. Claims 2-3, 14-15 and 26-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Vainio (Juha T. Vainio, "Bluetooth Security")* in view of *Kuwamoto et al. (EP 0919945)*.

45. *Vainio* teaches an ad-hoc radio communication as discussed above. *Vainio* does not explicitly teach that the verification data is visual and auditory verification data.

46. *Kuwamoto et al.* teach visual and auditory verification data [39].

47. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to utilize visual and auditory verification data in *Vainio's* invention given the benefit of usability.

48. In addition, the examiner also points out that the form of visual or auditory verification data are well known in the art. For example the correct transfer of data during synchronizing hand held devices (e.g. PALMS) with other devices (e.g. computers) is frequently verified by visual or auditory check of the sending and receiving device.

49. Claims 4, 6-8, 10, 12, 16, 18-20, 22, 24, 28, 32, 34, 39 and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Vainio (Juha T. Vainio, "Bluetooth Security")* in view of *Schneier (Bruce Schneier, "Applied Cryptography, Protocols, Algorithms and Source Code in C", 2nd edition, 1996 ISBN: 0471128457)*.

50. Vainio teaches a method and a system including a first generation algorithm (*E1*)

that given input of the data for verification data generation outputs the verification data as discussed above.

51. As per claims 4, 6-7, 16, 18-19 Vainio does not teach that the first generation algorithm comprise a serial sequence of operators that are composed of more than one operators arranged in series, wherein the operators relate to the same or different one-way function.

52. Schneier's discloses a serial sequence of operators that are composed of more than one operators arranged in series that are related to the same or different one-way function (*pg. 351-353 and 433-438*).

53. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate of more than one operators arranged in series that are related to the same or different one-way function as taught by Schneier into the first generation algorithm as taught by Vainio. One of ordinary skill in the art would have been motivated to perform such a modification in order to increase system's security.

54. As per claims 4, 6-7, 16, 18-19 Vainio does not teach the encryption E0 (*that* for verification data generation is operated by the serial sequence of operators

55. As per claims 8 and 20 Vainio does not explicitly teach transmitting a public key between the portable devices.

56. *Schneier* teaches transmitting a public key from a sender and a receiver to allow secure communication (*Alice and Bob, "2.5 Communications using public-key*

cryptography", pg. 31-32). However, *Schneier* warns about "man-in-the-middle attacks" (pg. 48-49).

57. Vainio teaches sending data for verification data generation (*RAND A*) from a sender to a receiver that allows generating verification data (*SRES*). The verification data is derived from additional data that is unique to the recipient (*Vainio Fig. 6*) and is sent back for verification to the sender. This scheme decreases chances of "man-in-the-middle attacks".

58. Thus, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to transmit the public key from one portable terminal to another as taught by *Schneier* as the data for verification data generation as taught by *Vainio*. One of ordinary skill in the art would have been motivated to perform such a modification in order to secure data exchange between portable terminals (*solving a key-management problem*) while minimizing man-in-the-middle attacks.

59. As per claims 10, 12, 22 and 24 *Vainio* teaches that one of the portable terminals receive information and using the information (*and second generation algorithms E21, E22*) produces a symmetric key *Kc* (*Fig. 2 and 3*). *Vainio* explicitly teach that *Kc* is produced on both portable terminals (*Vainio talks about the key exchange process, pg. 8*). The information comprise a random number (*RandD*) and it is implicit that they also must comprise information identifying the second generation algorithm in order for the key exchange parties to know which of the algorithms was used in order to derive the identical *Kc*.

60. Vainio does not explicitly teach that the Kc is sent from the portable terminal to the personal computer of each user and the personal computers exchanging data in cipher using the symmetric key Kc.

61. Official Notice is taken that it is old and well-known practice to communicate data from a portable terminal to a personal computer (*e.g. U.S. Pub. No. 20010013890*). One of ordinary skill in the art at the time of applicant's invention would have been motivated to extend personal computer's capability by data easily obtained using a portable device as well as extend the portable terminals that have limited resources such as memory.

62. Also Official Notice is taken that it is old and well-known practice to use personal computers to send and receive data in cipher using symmetric keys. One of ordinary skill in the art at the time of applicant's invention would have been motivated to employ secure data communication between personal computers.

63. *Schneier* teaches that the cipher key should be done using other communication channels than cipher data exchange (*Schneier, pg. 176, last three §-pg. 177, first two §*) and using portable terminals (*as taught by Vainio*) as "other communication channels" would have been an obvious choice given the benefit of portability and "man-in-the-middle" attack prevention mechanism.

64. Claims 9, 11, 21, 23, 33, 35, 38 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Vainio* (*Juha T. Vainio, "Bluetooth Security"*) in view of *Schneier* (*Bruce Schneier, "Applied Cryptography, Protocols, Algorithms and Source Code in*

C", 2nd edition, 1996 ISBN: 0471128457) and in further view *Lin* (U.S. Pub. 20020025046).

65. Claims 9, 11, 21 and 23 are essentially identical to claims 10, 12, 22 and 24 discussed above with the exception that the symmetric Kc is computed on the personal computers rather than portable terminals.
66. Lin teaches that computing power, memory capacity and supply power of the portable device may not be sufficient for key generation (*Lin*, [21]). Thus, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify Vainio's invention in order to generate the keys Kc on the personal computers. One of ordinary skill in the art would have been motivated to perform such a modification in order to move key generation into the higher power and memory capacity devices.
67. Claims 1-3, 8, 13-15, 20 and 25-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Vainio* (*Juha T. Vainio, "Bluetooth Security"*) in view of *Hind et al.* (U.S. Pub. No. 6772331).
68. As per claims 1, 13 and 25 *Hind et al.* teach sending data for verification data generation (certificate 6030) from one data send/receive device to the other send/receive device (6001/6003), wherein the two send/receive devices are mutually connected by an ad-hoc radio connection (col. 9 lines 16-20 and fig. 6) upon which verification data (*the identifier of the sending device*) is displayed and verified that matches mutually (col. 13 lines 17-26).

Art Unit: 2134

69. Hind et al. teach that the verification data is generated by a first generation algorithm
(col. 12 lines 3-5).

70. As per claims 2-3, 14-15 and 26-27- Hind et al. teach that the verification data is the
visual and auditory form (col. 13 lines 17-26).

71. As per claims 8 and 20 the data for verification data generation comprise public key
(fig. 4).

Conclusion

The prior art made of record and not relied upon is considered pertinent to
applicant's disclosure:


Hind et al. (U.S. Patent No. 6886095),

De La Huerga (U.S. Pub. No. 20020038392),

Luo (U.S. Patent No. 5909491),

Matsuzaki et al. (EP No. 0809379),

Iijima (U.S. Patent No. 5225664).



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

3/3/6
